

Amendment and Response

Applicant: Andrew M. Spencer

Serial No.: 10/689,157

Filed: October 20, 2003

Docket No.: 10013891-1

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION
KEY AND ENCRYPTION KEYS

IN THE CLAIMS

The pending claims are as follows:

1. (Original) A removable information storage device suitable for use with a host, comprising:
 - a non-volatile memory configured to store a master encryption key; and
 - a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys.
2. (Original) The information storage device of claim 1, further comprising an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key and to encrypt and decrypt the data using one or more of the encryption keys.
3. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a magnetic memory.
4. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a read-only memory which includes fuse elements.
5. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a nitrided read-only memory.
6. (Original) The information storage device of claim 1, wherein the first non-volatile memory is an erasable programmable read-only memory.

Amendment and Response

Applicant: Andrew M. Spencer

Serial No.: 10/689,157

Filed: October 20, 2003

Docket No.: 10013891-1

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION
KEY AND ENCRYPTION KEYS

7. (Original) The information storage device of claim 1, wherein the first non-volatile memory is an electronically erasable programmable read-only memory.
8. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a flash erasable programmable read-only memory.
9. (Original) The information storage device of claim 1, wherein the first non-volatile memory is a one time programmable read-only memory.
10. (Original) The information storage device of claim 1, wherein the non-volatile magnetic memory is a magnetic random access memory.
11. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.
12. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas.
13. (Original) The information storage device of claim 1, wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.
14. (Original) The information storage device of claim 13, wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory.
15. (Original) The information storage device of claim 13, wherein the first areas are located at one or more random address locations within the second non-volatile memory.

Amendment and Response

Applicant: Andrew M. Spencer

Serial No.: 10/689,157

Filed: October 20, 2003

Docket No.: 10013891-1

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION KEY AND ENCRYPTION KEYS

16. (Withdrawn) A portable memory card, comprising:
a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data; and
a card controller system coupled to the memory storage device configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device, wherein the encryption keys are encrypted and decrypted using a master encryption key and the data is encrypted and decrypted using the encryption keys.
17. (Withdrawn) The portable memory card of claim 16, wherein the non-volatile memory is a magnetic memory.
18. (Withdrawn) The portable memory card of claim 16, wherein the non-volatile memory is an atomic resolution storage memory.
19. (Withdrawn) The portable memory card of claim 16, wherein the card controller system includes a non-volatile master key memory configured to store the master encryption key.
20. (Withdrawn) The portable memory card of claim 16, wherein the card controller system includes an encryption and decryption engine configured to store one or more encryption algorithms and use the encryption algorithms to encrypt and decrypt the encryption keys using the master encryption key and encrypt and decrypt the data using the encryption keys.
21. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas.

Amendment and Response

Applicant: Andrew M. Spencer

Serial No.: 10/689,157

Filed: October 20, 2003

Docket No.: 10013891-1

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION KEY AND ENCRYPTION KEYS

22. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys and the encrypted data are stored in the first areas.

23. (Withdrawn) The portable memory card of claim 16, wherein the memory storage device is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the first and second areas.

24. (Withdrawn) A memory card, comprising:

- a non-volatile master key memory configured to store a master encryption key;
- an encryption and decryption engine configured to implement one or more symmetrical encryption key algorithms based on the master encryption key and encryption keys;
- a memory storage device comprising an atomic resolution storage device including a field emitter, a media and a micromover, the atomic resolution storage device configured to store the encryption keys after the encryption keys are encrypted using the master encryption key and to store data after the data is encrypted using the encryption keys;
- a host interface configured to provide a communication interface to a host;
- a memory interface configured to provide a communication interface to the memory storage device;
- a data path manager configured to manage communication of the data and the encrypted data between the host and the memory storage device; and
- a controller processor configured to control the encryption and decryption of the encryption keys using the master encryption key and the encryption and decryption of the data using the encryption keys.

25. (Withdrawn) An information storage device, comprising:

- a non-volatile memory storage device configured to store one or more encrypted encryption keys and encrypted data; and

Amendment and Response

Applicant: Andrew M. Spencer

Serial No.: 10/689,157

Filed: October 20, 2003

Docket No.: 10013891-1

Title: REMOVABLE INFORMATION STORAGE DEVICE THAT INCLUDES A MASTER ENCRYPTION KEY AND ENCRYPTION KEYS

controller means configured to store and retrieve the encrypted encryption keys and the encrypted data from the memory storage device and to encrypt and decrypt the encryption keys using a master encryption key and to encrypt and decrypt the data using the encryption keys.

26. (Withdrawn) The information storage device of claim 25, wherein the controller means includes a non-volatile master key memory configured to store the master encryption key.

27. (Original) A method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

- providing the encryption keys to the information storage device;
- reading a master encryption key from a non-volatile memory;
- encrypting each one of the encryption keys using the master encryption key; and
- writing the encrypted encryption keys to a random access memory.

28. (Original) A method of decrypting encryption keys in an information storage device, comprising:

- reading the encrypted encryption keys from the magnetic random access memory;
- reading a master encryption key from a first non-volatile memory; and
- decrypting each one of the encryption keys using the master encryption key.

29. (Original) The method of claim 28, comprising:

- reading encrypted data from the magnetic random access memory; and
- decrypting the encrypted data using the encryption keys.

30. (Original) The method of claim 28, comprising:

- encrypting the data using the encryption keys; and
- writing the encrypted data to the magnetic random access memory.